PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification : Not classified

A2

(11) International Publication Number: WO 98/54943

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/EP98/02995

(22) International Filing Date: 12 May 1998 (12.05.98)

(30) Priority Data:
9709748.9 14 May 1997 (14.05.97) GB

(71)(72) Applicant and Inventor: HO KEUNG, Tse [GB/CN]; P.O. Box 54670, North Point Post Office, Hong Kong (CN).

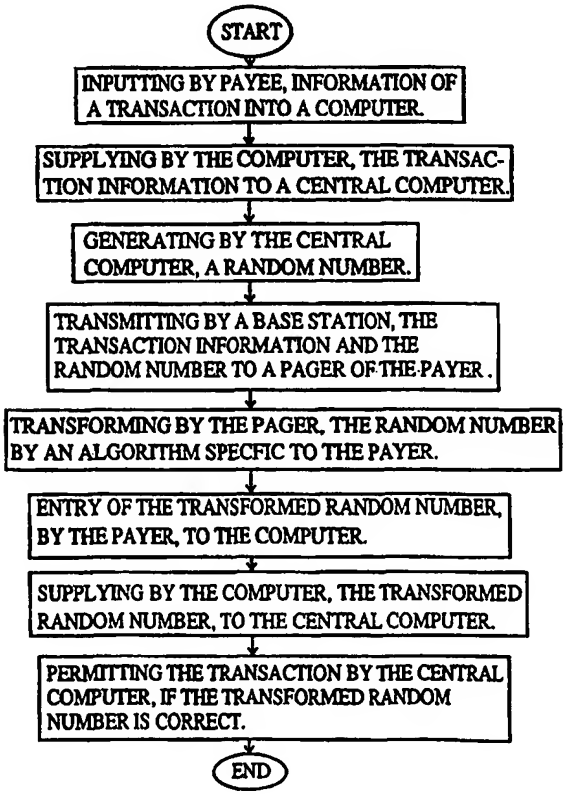
(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, US, VN, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: UNIVERSAL ELECTRONIC TRANSACTION SYSTEM AND METHOD THEREFOR

(57) Abstract

A pager for receiving information of a transaction and information which bears a predetermined relationship to a one–time, non–predictable code; and for conveying the information and the code to its user. The user, after checking the transaction information being correct, sends the code to a control centre directly or through the payee.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BNSDOCID: <WO___9854943A2_I_>

UNIVERSAL ELECTRONIC TRANSACTION SYSTEM AND METHOD THEREFOR

Field of the invention

The present invention relates to electronic transaction systems, and particularly, to an electronic money transaction system with high portability and flexibility for enabling user to effect transactions of any kinds or for any purposes.

Background of the invention

Nowadays, electronic money transaction systems are easily found in the services/products providers such as restaurants and shops for receiving payments. Among such conventional systems, the IC credit card is regarded as a comparatively secure means for effecting transactions, and even so, it does have a problem as lacking the capability of providing reliable information of the transaction to be authorised, and as a consequent, there is no guarantee that a transaction being authorised is exactly the transaction being intended by its holder.

In such a conventional system, a terminal is necessary to be disposed in the service/product provider for interfacing the IC card and coupling it to a remote central computer responsible for authenticating the IC card, by establishing a communication link. It should be noted that, the communication link need not be a secure one as far as communication between the IC card and central computer is concerned because when an authentication process takes place, the central computer will generate and send a random number to the IC card through the communication link, and the IC card will encrypt the random number and return the encryption result back to the central computer through the communication link. If the encryption result is correct, the central computer will permit the transaction. If a secure communication between the IC card and the central computer is to be used, this will only mean that the random number will be encrypted one more time, this should be unnecessary and even if it was necessary, it should be carried out by/inside the IC card instead.

However, the communication link has to be secure to ensure the transaction information communicated to the central computer cannot be intercepted and modified. Further, the terminal also have to be a secure device in order to provide reliable transaction information, particularly, the transaction amount, to the cardholder by means of , for e.g., a display. These increase the cost of the system and also cause other problems ...

To ensure no card fraud by, for e.g., the cashier of a services/products provider or even the provider itself, a IC card holder has to get into close vicinity of the terminal to monitor the transaction procedure handled by the cashier and desirably, should insert and remove the card into and from the terminal on his own.

In situations where such a terminal does not exist, the IC card will become useless, or it may take the card holder walk a long way if the location of the terminal is remote from the location where the cardholder receives the service/product, this may happen in a shop or restaurant with thousands of sq. ft. in size.

It may also be necessary for a cardholder to get out of his car to make payment for car park fee or fuel intake.

Finally, an I.C. card cannot be used for purchasing in internet environment.

Objects of the present invention :

Accordingly, it is therefore an object of the present invention to provide an apparatus to a user, rather than to the services/products providers, for conveying to the user directly reliable information of a transaction to be authorised, and for enabling the user to authorise that transaction; and a method therefor.

It is therefore another object of the present invention to provide an apparatus to a user, rather than to the services/products providers, for enabling an electronic transaction to take place with the aid of an inexpensive, non-secure communication link such as any existing general purpose communication(s) network system e.g.,

BNSDOCID: <WO___9854943A2_I_>

telephone, internet computer or the like, without modification thereof for the security problems as mentioned above; and a method therefor.

It is therefore a further another object of the present invention to provide a universal electronic transaction system which being low cost, secure, not dedicated for any particular purpose; and a method therefor.

Brief description of the invention:

According to one embodiment of the present invention, there is provided a pager for receiving a paging signal representative of information of, for e.g., a transaction on a user account, to be authorised, and representative of a one time, non-predictable code for use by the user to authorise that transaction. The user of the pager, after checking the transaction information including transaction amount and payee's identity, being correct, sends or gives the one time, non-predictable code to the payee who will communicate the one time, non-predictable code to the bank for authorising the transaction.

According to another embodiment of the present invention, there is provided a pager with an IC card receiving port therein for receiving an external conventional IC credit card. The pager being for receiving a paging signal representative of information of a transaction to be authorised and representative of a random number. The IC card being for transforming the random number according to an encryption algorithm specified to the user to a one time, non-predictable code which being for use by the user to authorise that transaction.

Brief description of drawing

FIG.1 is a block diagram of a present paging receiver according to a first embodiment.

FIG.2 is a flow chart of a method for a present authorisation process.

Detailed description of the preferred embodiments

Referring to Fig.1, there is shown a block diagram of a paging receiver 1, according to a first embodiment of the present invention, in which comprising :

1) a receiver circuit 23 for receiving paging signals, including signals representative of electronic money transaction information (herein below referred as E signals) ;

2) an address comparator 25 for determining whether a signal received is assigned to paging receiver 1 and may comprise a plurality of addresses for reception of corresponding different kinds of signals ;

3) a CPU 21 for fetching a message following the call signal is determined to be assigned to the receiver 1 by address comparator 25 ;

4) a message memory 28 for storing received messages of signals assigned to paging receiver 1;

5) a display 34 for displaying the message received ;

6) a cryptographic algorithm memory 27 containing cryptographic algorithm(s) for transforming at least a part of the E signals, of which details will be described herein below later ;

7) a speaker 33 and led 31 for providing sound and light signal respectively to a user for indicating a paging signal assigned to paging receiver 1 received .

When in operation, the paging receiver 1 will receive any paging signals transmitted from a base station of the same pager based broadcast system. Such a paging signal contains 4 fields, namely as, 1) address field for containing an address of the paging receiver assigned for receiving the signal ; 2) type field for indicating whether the signal is a E signal or not ; 3) information field for containing information to be displayed to user ; 4) signal number identity for indicating to the assigned paging receiver that, a signal which being broadcasted by the base station more than one time for ensuring it will be received by the assigned paging receiver, be the same signal, so that the assigned pager receiver will ignore the successively identical signals and will not alert the user unnecessarily. The receiving circuit 23, after

BNSDOCID: <WO___9854943A2_I_>

amplifying the incoming paging signal, supplies the signal to the address comparator 25 which will compare the address field of the signal with one or a number of stored address(es) therein, and if a coincidence occurs, the address comparator will feed the rest of the signal to the CPU 21, otherwise, the rest of the signal will be ignored.

According to the first embodiment, the present paging receiver is for authorisation of transactions. Referring to Fig.2, which is a flow chart of a method for the authorisation process. As read on Fig.2, when an authorisation process takes place, an internet computer receives the account number of a user. Desirably, the internet computer has a card reader therein for obtaining the user account number by, for instance, reading a magnetic card or a IC card or the like of the user, otherwise the user account number will have to be entered by hand with the aid of a keyboard. Then, the internet computer supplies the account number together with the transaction information, which may be entered into the computer with the aid of a keyboard by the payee/payer and which may include information such as identity of payee, transaction amount, purpose of payment, e.g., deposit or full payment for a particular product or service or the like, identity of product(s) and services concerned etc., to a central computer via a communication link which in this case, the internet. The central computer, in response thereto, generates a random number which being a random number and searches in a storage thereof the user identity corresponding to the user account number received and then supplies the user identity searched, the transaction information received together with the random number to the base station mentioned above.

The base station will then search in an address storage thereof an address of the paging receiver, corresponding to the user identity received, and generate a paging E signal, in a format as mentioned above and in which the information field contains the transaction information and the random number, and broadcast the signal.

The paging receiver 1, after receiving the signal, transforms the random number therein by using an algorithm which being specific to the user and stored in

cryptographic algorithm memory 27, the result will be used as a one time, non-predictable code for authorising the transaction. Then, alerts the user and displays the transaction information and the code to the user. The user, after seeing that the transaction information being correct, enters the code read on display 34 into the keyboard of the internet computer which again sends it to the central computer.

The central computer, in response thereto, searches in a cryptographic algorithm storage thereof a cryptographic algorithm corresponding to the user identity and transforms the random number it generated previously by using the cryptographic algorithm searched and compared the result with the a one time, non-predictable code received, and if the comparison result is favourable, the transaction is determined as authorised.

It should be noted that the cryptographic process in the paging receiver 1 and the central computer may be omitted to simplify the authorisation process and at the same time, it can still provide an acceptable degree of security. This is possible for the reason that although theoretically, the paging signal is receivable by anyone, other people can actually not be able to receive it unless they know the correct address of the paging receiver 1 because nowadays, thousands of similar signals may occur and be receivable at the same instant of time.

On the other hand, to enhance the security, the paging receiver may includes a keypad thereon for receiving, by CPU 21, a password and without it CPU 21 will not perform the cryptographic process. Alternatively, it may also be desirable that once a password is entered, CPU 21 will perform the cryptographic process on the random numbers of E signals received within a predetermined period of time thereafter, or will perform the cryptographic process on the random numbers of any E signals until the total transaction amount of authorised transactions exceeds a predetermined value, so that the user need not to enter the password every time a transaction take place.

Further, the E signal may be modified into 2 separated signals, 1) E1 signal which being similar to the E signal as mentioned above, except that it contains

BNSDOCID: <WO___9854943A2_I_>

transaction information but no random number therein ; 2) the random number signal for containing the random number which being disguised as an ordinary telephone number. And, the address comparator 25 may contains a specific address dedicated for receiving the random number signal. In the random number signal, there is no type field for indicating to CPU 21 that it being a part of a E signal or the type field therein will not indicates it as a E signal, instead, the address comparator 25 will interrupt CPU 21 in a specific manner when it detects a received signal having an address in the address field thereof match the specific address, that is, a random number signal, thereby informing CPU 21 of this fact.

It should be noted that the specific address is different in different present paging receiver.

According to another embodiment of the present invention, there is provided a pager with an IC card receiving port therein for receiving an external conventional IC credit card. Similar to the first embodiment, the pager is also for receiving a paging E signal containing information of a transaction to be authorised on a user's bank account, or the like, and a random number, but in this case, the CPU 21 in the pager will not perform an cryptographic process on the random number, instead, it supplies it to the external IC card in the receiving port. The IC card, upon reception of the random number, will transform it according to an cryptographic algorithm therein, and the result will be used as a one time, non-predictable code, as mentioned above, and will be communicated to CPU 21 which will cause it, together with the transaction information received, to be displayed in display 34.

It should be noted that, as the user relies on the transaction information received by his pager in making a transaction, it is therefore no longer necessary or a must for the services/products providers to install a secure terminal as mentioned above. Rather, an existing general purpose communication(s) network system can be used for communicating the transaction information as well as the non-predictable

code for authorising the transactions to the central computer, and the central computer can be publicly accessible.

If merely communicating the account numbers of the money payer and receiver as well as the transaction amount is required, then using touch tone buttons on a telephone will be sufficient.

If further details of the transaction information is required, such as the purpose of the transaction, e.g. to purchase a Benz, model # 380s, serial # 1234 or even personal loan etc., then the transaction information may be communicated to an operator of the bank, who will be responsible for the data entry of the transaction information by means of a keyboard. In this case, it is desirable that both the money payer and receiver to have a respective pager of their own for receiving the transaction information and a different one time, non-predictable code for use by them respectively to authorise the transaction, so as to prevent loss to any one of them should there are errors in data entry.

It should be noted that the above embodiments are given by way of example only, and it will be obvious to those skilled in the art that various changes and modifications may be made without departing from the spirit of the present invention.

For instance, the transaction information may be encrypted by the central computer before transmitting to the pager. This can eliminate the possibility of the reception of E signal by the pager be interfered by an extremely strong disturbance signal and the pager be fooled by another fake E signal with the same random number therein but a false transaction information.

BNSDOCID: <WO___9854943A2_I_>

What is claimed is :

1) A secure transaction system, comprising :

A receiver with no transmitting capability, comprising :

means for receiving broadcasting signals assigned to said receiver, including a first signal representative of a non-predictable code associated with and dedicated for an attempted transaction and a second signal representative of information concerning said attempted transaction ;

means for conveying said information and said code to a user ;

wherein response from said user including said code is to be communicated to a control unit at least in part via a publicly accessible data communication medium for directing said attempted transaction ;

said control unit.

2) A system as claimed in claim 1, wherein there is a human operator for reception of said code through said publicly accessible data communication medium from another person, and for communication of said code to said control unit by means of an information input means.

3) A system as claimed in claim 1, wherein said second signal being in an encrypted form and said receiver will decrypt it before conveying it to said user.

4) A system as claimed in claim 1, wherein further comprising means for transforming said first signal by means of a predetermined cryptographic algorithm specific to said user, thereby obtaining said code from said first signal.

5) A system as claimed in claim 1, wherein said receiver is a paging receiver.

6) A system as claimed in claim 5, wherein said first signal is disguised as paging signal representative of a telephone number.

7) A system as claimed in claim 1, wherein said publicly accessible data communication medium being a telephone network and said code being entered by means of touch tone buttons on a telephone.

8) A system as claimed in claim 1, wherein said publicly accessible data communication medium being the internet and said code being entered by means of an internet computer.

9) A system as claimed in claim 1, wherein said receiver further comprising a means for receiving an external module for transforming said first signal by means of a predetermined algorithm specific to said user, thereby obtaining said code .

10) A system as claimed in claim 1, wherein said means for conveying being a display.

11) A system as claimed in claim 1, wherein said transaction being an electronic money transaction on an account of said user.

12) A system as claimed in claim 1, wherein said control unit will determine said attempted transaction as being approved by said user, if said code is being received.

13) A system as claimed in claim 1, wherein said control unit will determine said attempted transaction as being conducted by said user, if said code is being received.

BNSDOCID: <WO___9854943A2_I_>

14) A secure transaction system, comprising :

means for generating a first signal representative of a one time, non-predictable code ;

means for broadcasting a second signal representative of information concerning an attempted transaction and said first signal to a receiver of a user who has the authority or right to conduct the attempted transaction, said receiver has no transmitting capability ;

means for receiving response from said user containing said one time, non-predictable code therein at least in part via a publicly accessible data communication medium ;

means for using said user response to direct said attempted transaction .

15) A system as claimed in claim 14, wherein further comprising said receiver which being a paging receiver.

16) A system as claimed in claim 14, wherein said second signal being in an encrypted form and said receiver will decrypt it before conveying it to said user.

17) A system as claimed in claim 14, wherein said receiver transforms said first signal by means of a predetermined cryptographic algorithm specific to said user, thereby obtaining said one time, non-predictable code from said first signal.

18) A method for securely conducting transactions, comprising :

generating, by a control unit, a first signal representative of a non-predictable code ;

associating said first signal with an attempted transaction ;

transmitting a second signal representative of information concerning said attempted transaction and said first signal to a receiver of a user who has the authority or right to conduct said attempted transaction, said receiver has no transmitting capability ;

conveying, by said receiver, said information and said code to said user ;

wherein said code is for use by said user to make a response, to cause the transaction to be completed .

19) A method as claimed in claim 18, wherein further comprising the steps of communicating said code back to said control unit at least in part via a publicly accessible data communication medium ; determining , by said control unit, said attempted transaction as being conducted by said user if said code is being received.

20) A system for securely conducting transactions in situations where communication link to a control unit is already provided by a service/product provider for communicating information of a requested transaction or the like to said control unit, and a communication between the purchaser of said requested transaction and said service/product provider exists, comprising :

A portable receiver of said purchaser, which has no transmitting capability, comprising :

means for receiving broadcasting signals assigned to said receiver, including a first signal representative of a non-predictable code associated with and dedicated for said requested transaction and a second signal representative of information concerning said requested transaction ;

means for conveying said information concerning said requested transaction and said code to said purchaser ;

BNSDOCID: <WO___9854943A2_I_>

wherein a user response having said code therein is to be communicated to a control unit at least in part via a publicly accessible data communication medium for approving said requested transaction ;

and said control unit.

21) A system as claimed in claim 20, wherein said information concerning said requested transaction includes said information of a requested transaction.

22) In a system for securely conducting transactions, a receiver with no transmitting capability, comprising :

means for receiving broadcasting signals assigned to said receiver, including a first signal representative of a code associated with and dedicated for an attempted transaction and a second signal representative of information concerning said attempted transaction ;

means for conveying said information and said code to a user ;

wherein said code is for use by said user to cause said transaction to be completed.

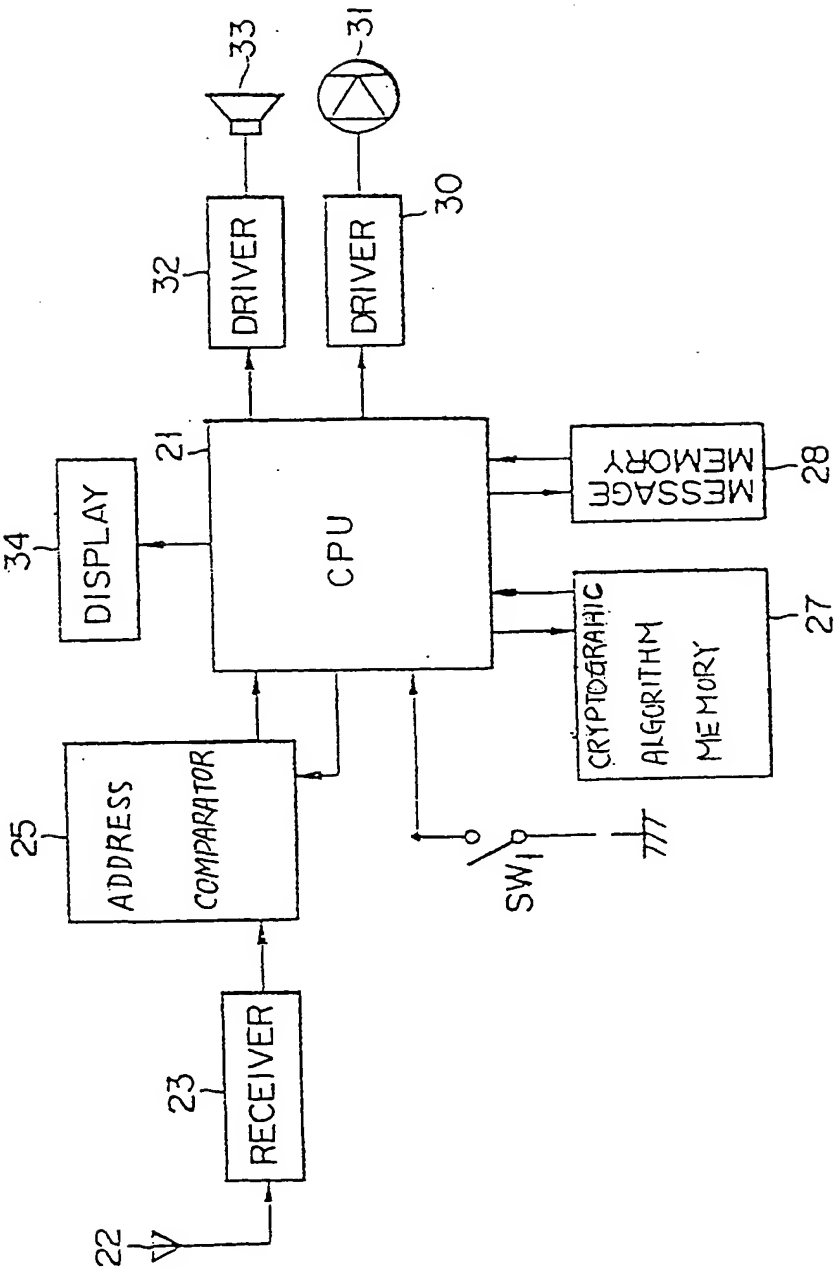
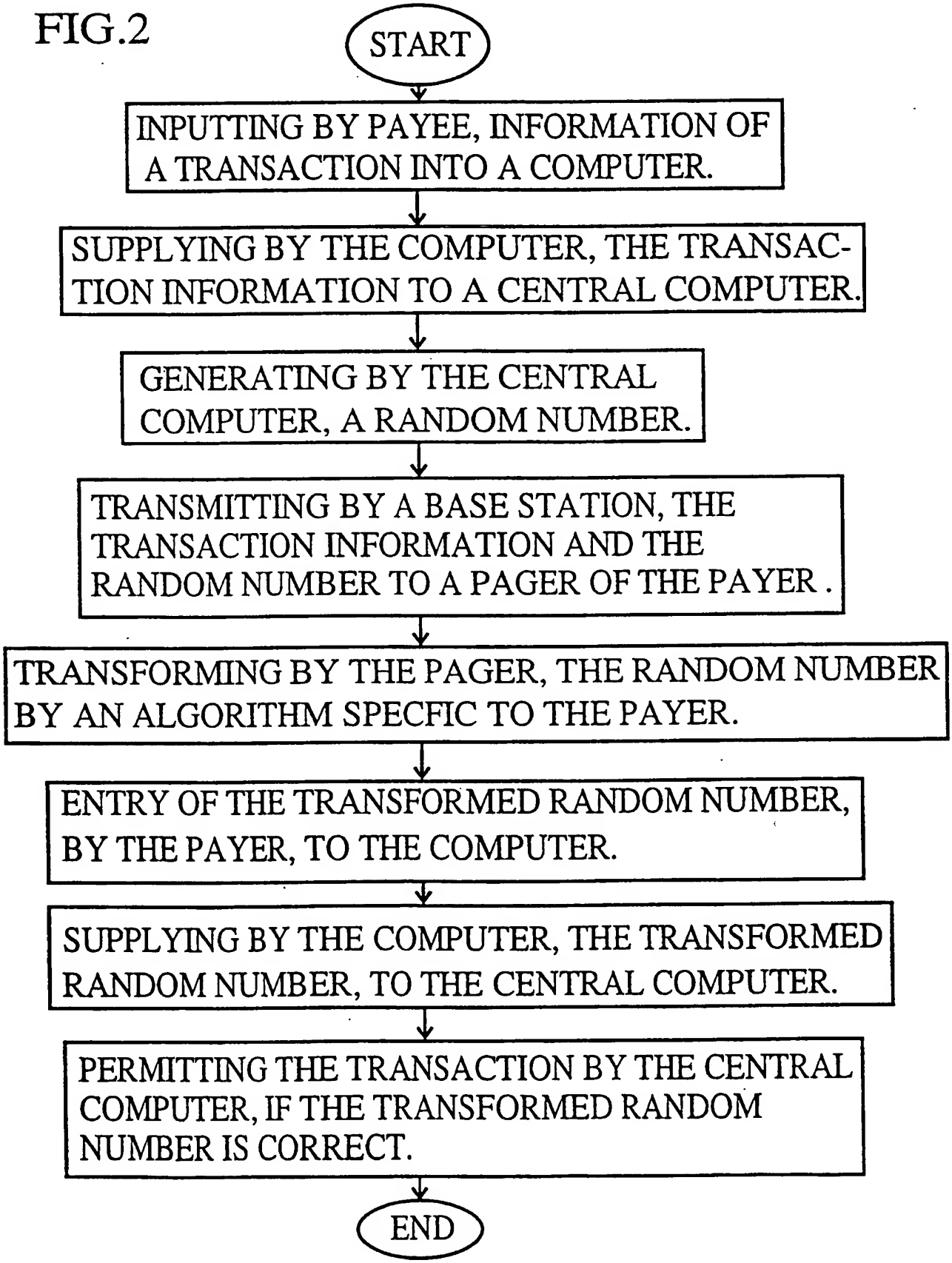


FIG. 1

ENSDOCID: <WO___9854943A2_I_>

FIG.2


START
INPUTTING BY PAYEE, INFORMATION OF A TRANSACTION INTO A COMPUTER.
SUPPLYING BY THE COMPUTER, THE TRANSACTION INFORMATION TO A CENTRAL COMPUTER.
GENERATING BY THE CENTRAL COMPUTER, A RANDOM NUMBER.
TRANSMITTING BY A BASE STATION, THE TRANSACTION INFORMATION AND THE RANDOM NUMBER TO A PAGER OF THE PAYER .
TRANSFORMING BY THE PAGER, THE RANDOM NUMBER BY AN ALGORITHM SPECFIC TO THE PAYER.
ENTRY OF THE TRANSFORMED RANDOM NUMBER, BY THE PAYER, TO THE COMPUTER.
SUPPLYING BY THE COMPUTER, THE TRANSFORMED RANDOM NUMBER, TO THE CENTRAL COMPUTER.
PERMITTING THE TRANSACTION BY THE CENTRAL COMPUTER, IF THE TRANSFORMED RANDOM NUMBER IS CORRECT.
END

THIS PAGE BLANK (USPTO)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10

A3

(11) International Publication Number: WO 98/54943

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/EP98/02995

(22) International Filing Date: 12 May 1998 (12.05.98)

(30) Priority Data:
9709748.9 14 May 1997 (14.05.97) GB

(71)(72) Applicant and Inventor: HO KEUNG, Tse [GB/CN]; P.O. Box 54670, North Point Post Office, Hong Kong (CN).

(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, US, VN, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

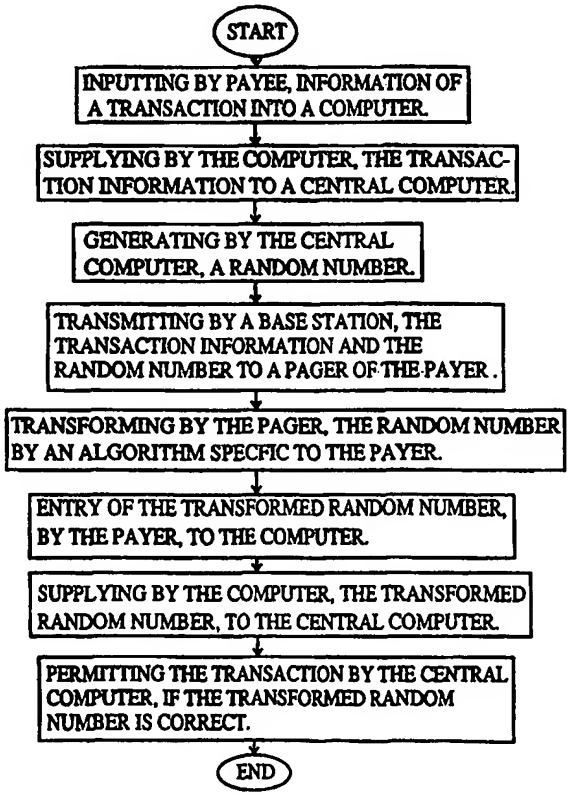
Published
With international search report.

(88) Date of publication of the international search report:
29 July 1999 (29.07.99)

(54) Title: UNIVERSAL ELECTRONIC TRANSACTION SYSTEM AND METHOD THEREFOR

(57) Abstract

A pager for receiving information of a transaction and information which bears a predetermined relationship to a one–time, non–predictable code; and for conveying the information and the code to its user. The user, after checking the transaction information being correct, sends the code to a control centre directly or through the payee.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BNSDOCID: <WO___9854943A3_I_>

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/EP 98/02995

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 745 961 A (AT & T CORP) 4 December 1996 see claim 1; figure 1	1,2,5-7, 9-13,22 3,4,8, 14-21
A	US 5 285 496 A (FRANK EDWARD H ET AL) 8 February 1994 see claim 1; figure 1A	1-22
A	US 5 521 966 A (FRIEDES ALBERT ET AL) 28 May 1996 see claim 1; figure 1	1-22
A	US 5 483 595 A (OWEN JEFFREY R) 9 January 1996 see claim 1; figure 1	1-22

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 May 1999	19/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/EP 98/02995

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0745961 A	04-12-1996	US 5708422 A	13-01-1998
		CA 2176163 A	01-12-1996
		JP 8339407 A	24-12-1996
US 5285496 A	08-02-1994	NONE	
US 5521966 A	28-05-1996	CA 2118547 A,C	15-06-1995
		CN 1120202 A	10-04-1996
		EP 0658862 A	21-06-1995
		JP 7200425 A	04-08-1995
		SG 52575 A	28-09-1998
US 5483595 A	09-01-1996	NONE	

BNSDOCID: <WO___9854943A3_I_>

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10

A3

(11) International Publication Number: WO 98/54943

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/EP98/02995

(22) International Filing Date: 12 May 1998 (12.05.98)

(30) Priority Data:
9709748.9 14 May 1997 (14.05.97) GB

(71)(72) Applicant and Inventor: HO KEUNG, Tse [GB/CN]; P.O. Box 54670, North Point Post Office, Hong Kong (CN).

(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SK, UA, US, VN, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG)

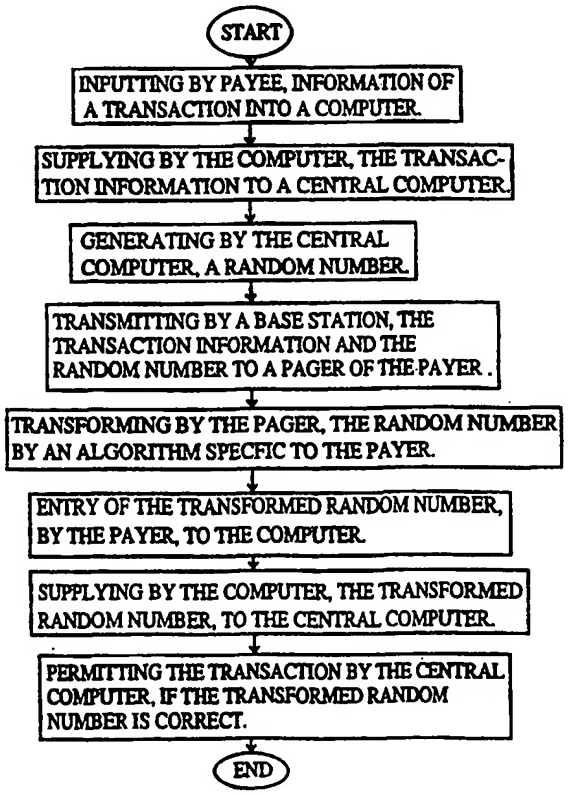
Published
With international search report.

(88) Date of publication of the international search report:
29 July 1999 (29.07.99)

(54) Title: UNIVERSAL ELECTRONIC TRANSACTION SYSTEM AND METHOD THEREFOR

(57) Abstract

A pager for receiving information of a transaction and information which bears a predetermined relationship to a one–time, non–predictable code; and for conveying the information and the code to its user. The user, after checking the transaction information being correct, sends the code to a control centre directly or through the payee.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BNSDOCID: <WO___9854943A3_IA>